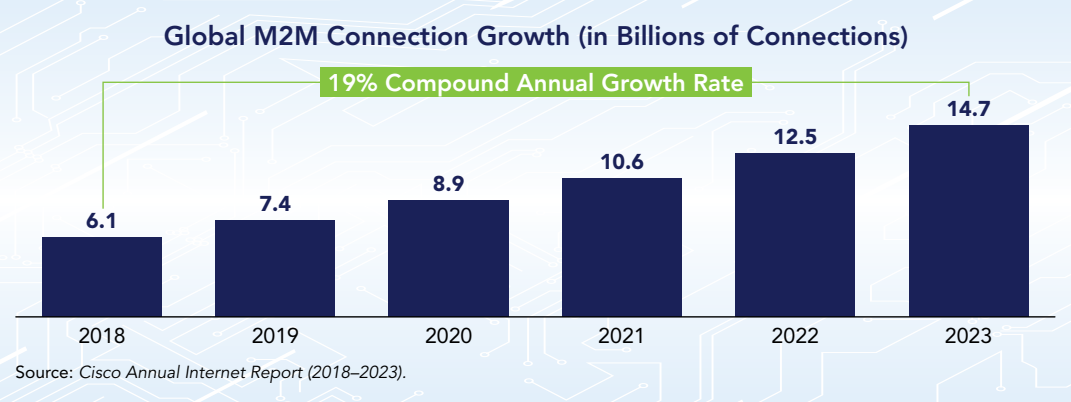
BSA Policy Principles for Building a Secure and Trustworthy Internet of Things

The evolving nature of the internet is creating new opportunities to connect devices, applications, and services on a scale that will transform daily interactions with our physical environment, work, and society. The Internet of Things (IoT) carries enormous potential to change the world for the better. Projections for the impact of the IoT on the internet and the global economy are significant, forecasting explosive growth in the number of IoT devices and their use in various applications. Globally, machine-to-machine (M2M) connections, which include IoT, will more than double in the coming years, from 6.1 billion in 2018 to 14.7 billion by 2023.[1]



Source: *Cisco Annual Internet Report (2018–2023).*

Globally, machine-to-machine (M2M) connections, which include IoT, will more than double in the coming years, from 6.1 billion in 2018 to 14.7 billion by 2023.

Billions of IoT devices, applications, and services are already in use, with more coming online each day, and every new device can expand opportunities for malicious actors to disrupt the digital ecosystem. Some estimates conclude that cyberattacks on IoT devices in the first half of 2019 increased by 300 percent compared to the second half of 2018.[2] As the IoT continues to grow, IoT security is therefore of the utmost importance.

---

[1] Cisco, *Cisco Annual Internet Report (2018–2023)*, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

[2] F-Secure, *Attack Landscape H1 2019*, https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf; see also Zak Doffman, "Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims," *Forbes* (September 14, 2019), https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#220ecd435892.

Inadequately secured IoT devices and services can serve as entry points for cyberattacks, compromising sensitive data and threatening the safety of individual users. Attacks on infrastructure and other users, fueled by networks of poorly secured IoT devices, can affect the delivery of essential services such as health care and basic utilities, put the security and privacy of others at risk, and threaten the resilience of the internet globally.

These challenges provide ample reason to bring together governments and the technology industry to increase the security of the IoT. Policymakers must take action to create spaces where challenges can be explored, and solutions identified.

As trusted leaders in the global software industry, BSA members are at the forefront of IoT innovation, including advancements in IoT security. BSA endorses a series of principles for building trust in the IoT that embody a responsible, risk-based approach to government IoT security policy.

BSA IoT SECURITY POLICY PRINCIPLES

Governments should develop IoT security policies that:

1. Account for the IoT ecosystem's diversity and complexity.
2. Define key concepts and requirements clearly.
3. Secure the whole IoT ecosystem, not just devices.
4. Distinguish between consumer IoT and industrial IoT (IIoT).
5. Build on industry best practices.
6. Incentivize security throughout the IoT life cycle.
7. Embrace multi-stakeholder processes.
8. Seek national and international policy harmonization.
9. Support development and use of internationally recognized IoT standards.
10. Establish baseline security requirements as necessary and appropriate.
11. Integrate security into IoT acquisition.
12. Include IoT in incident response.

IoT Security Policies Should Account for the IoT Ecosystem's Diversity and Complexity

Though there is no widely accepted, singular definition of IoT, the term generally describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

IoT systems often include device elements, such as sensors and actuators, data processors, and user interfaces, and network elements, like gateways and cloud infrastructure.

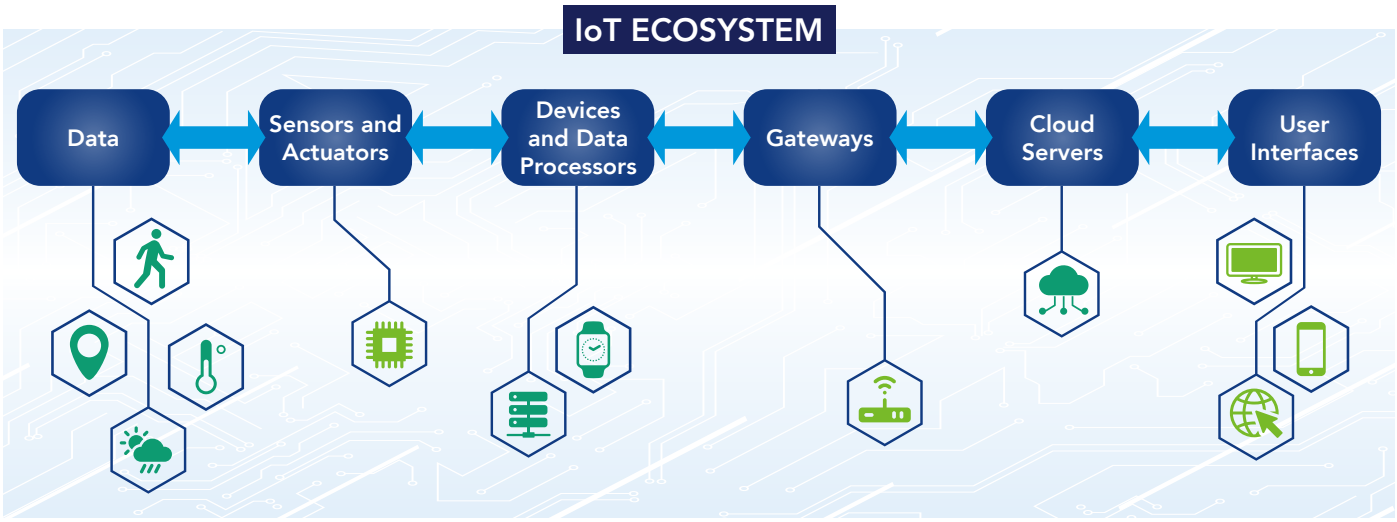
KEY ELEMENTS

IoT Devices. IoT devices can connect to and are in regular connection with the internet, and have computer processing capabilities that can collect, send, or receive data. IoT devices may incorporate user interfaces, data processors, and potentially multiple sensors—for example, IoT devices can contain GPS, accelerometer, and camera sensors. Devices may be complex systems, such as programmable logic controllers, or may be so simple that they have no operating system.

- **Sensors and Actuators.** Sensors collect data from the surrounding environment. This collected data can have varying degrees of intricacy, ranging from simple temperature monitoring to a complex video feed. Actuators receive information from sensors and turn it into physical action, such as prompting an electric motor or hydraulic system to activate.
- **Data Processors.** Data processors refer to components that perform operations to covert data into useful insights, which can be interpreted and used for analysis. Data processing functions can range from simple, such as checking that pressure readings are within an acceptable range, to complex, like identifying objects in a video using computer vision.
- **User Interfaces.** User interfaces consist of features through which end users interact with the IoT system, including screens, pages, buttons, forms, icons, and text. User interfaces are closely related to the user experience, the interactions a user has with a product and the portals or applications used to remotely manage IoT devices.

Networks. Networks allow data collected by IoT devices to be transported to a cloud infrastructure. IoT devices can be connected to the cloud through various mediums of communication and transports, such as cellular networks, satellite networks, Wi-Fi, Li-Fi, and Bluetooth. 5G networks, with new edge computing capabilities, will create myriad new possibilities for the use and management of IoT devices. Related to networks, gateways and cloud infrastructure are other important components of the IoT ecosystem.

- **Gateways.** Gateways manage data traffic between IoT devices and the networks to which they connect. They may include hardware and/or software elements; for example, in a home environment, a router often serves as a gateway between the home Wi-Fi network and the internet service provider. Gateways can be configured to perform pre-processing of the collected data from thousands of sensors locally before transmitting it to the next stage. Another gateway function is to translate different network protocols and make sure connected devices and sensors are interoperable. Gateways can also offer a certain level of security for the network and transmitted data with higher order encryption techniques. It acts as a middle layer between devices and the cloud to protect the system from malicious attacks and unauthorized access.
- **Cloud Infrastructure.** Cloud infrastructures refer to distributed computing and database management systems optimized to efficiently handle massive amounts of data. Cloud servers offer tools to collect, process, manage, and store large amounts of data in real-time, integrating inputs from many sensors, devices, gateways, and protocols. They also enable the creation of virtual or containerized environments in which customized security controls and other rules can be applied to a specified group of systems, creating powerful tools for IoT device management.



These various components illustrate that the IoT is not a monolith, but rather a complex system of different devices, communication networks, interfaces, and people. Complex supply chains, potentially including many third parties, make security evaluations challenging and require that systems be secured holistically with coordination among different parties and parts of the system. Moreover, the IoT includes elements, such as cloud services and telecommunications networks, that may be subject to other policy regimes.

Governments should holistically consider the complexity and diversity of the IoT ecosystem, recognizing the unique role each part of the system plays and how those parts interact, and design policies that are technology-neutral and flexible to accommodate such complexity. Moreover, IoT security policies must be aligned and comport with security policies impacting various elements of the IoT ecosystem, such as cloud and 5G security.

IoT Security Policies Must Define Key Concepts and Requirements Clearly

As governments formulate IoT security policies, policymakers must ensure technical definitions and security requirements are clearly defined. Specific, understandable definitions that follow international, consensus-driven, widely adopted standards for key terms, such as "IoT" and "IoT device," are critical to clearly communicating policies' scope and intent to consumers, industry, and other stakeholders, and to avoiding the creation of fragmented definitions. Similarly, security requirements within IoT security policies must be clearly defined. If policymakers choose to require specific security measures, these policies should create proper incentives for manufacturers to adopt established international standards that outline such capabilities and protocols that are appropriate and reasonable (e.g., at the International Organization for Standardization or International Electrotechnical Commission), and avoid codifying today's capabilities and practices, which may become quickly outdated. Clearly communicated, user-friendly IoT security policies ensure that consumers can easily understand device security practices and features, and that IoT manufacturers and vendors can efficiently address security priorities. Key definitions and requirements in IoT security policies are often overly broad or omitted entirely, creating confusion for consumers and businesses.

Clearly communicated, user-friendly IoT security policies ensure that consumers can easily understand device security practices and features.

Governments must clearly define key concepts and requirements related to IoT security consistent with international norms to the greatest extent possible.

DEFINING "IoT DEVICE"

Policymakers should ensure IoT security policies define which devices are covered with the greatest specificity and clarity possible. In general, IoT security policies should use a definition for "IoT device" that:

- Refers to a device that is designed to connect to a network and includes computer processing capabilities necessary to collect, send, or receive data;
- Refers to a finished product available to end users that is usable for its intended functions without being embedded or integrated into any other product and is not a component [It is possible that some IoT devices may be used within larger systems, which together constitute a composite IoT device (consider a "smart bus" that itself has many connected IoT devices, such as a connected camera or connected digital display, inside of it), but even in such composite IoT devices, any incorporated device must be able to function separately to be considered an IoT device itself];
- Acknowledges that IoT devices are designed to be connected to a broader ecosystem that includes other components, devices, and systems; and
- Does not include general computing devices, including personal computing systems, smart mobile communications devices, and mainframe computing systems.

Increasingly, innovative approaches to securing IoT devices depend on technologies or methodologies that are not device-based.

IoT Security Policies Should Secure the Whole IoT Ecosystem, Not Just Devices

Depending on the operating environment, many different risk-based approaches exist that achieve desired security outcomes. Increasingly, innovative approaches to securing IoT devices depend on technologies or methodologies that are not device-based. In some cases, these approaches may substitute for device-centric security measures.

Many efforts to develop IoT security guidance have been narrowly focused on device characteristics. Security approaches that consider the ecosystem perspective suggest that IoT device security best practices are undoubtedly important, but equally important is the security of all the elements in the IoT system. Moreover, security efforts must be aligned: policymakers must ensure that device-centric security policies do not undermine the ability of vendors and customers to innovate and apply extra-device security measures. For example, policies should avoid password requirements for IoT devices that interrupt single sign-on identity management technologies that improve both security and user experience.

Similarly, many security experts argue all IoT devices should be able to receive secure patches or updates. This feature enables vendors to better maintain their devices, including mitigating discovered vulnerabilities, but can bring trade-offs in terms of the cost, time-to-market, and complexity of the device. However, device capabilities may be limited due to use requirements that may prevent the implementation of such

features. One emerging alternative is the creation of customized cloud environments to which administrators can apply security rules tailored to the devices managed within the environment—including applying "virtual patches" that mitigate particular device vulnerabilities without the need to install new software on the device itself.

Another example is the "Manufacturer's Usage Description" (MUD), a protocol that enables devices to communicate critical information to routers to enable their secure management. In this case, devices—which contain a software tag listing information about the device's data, communication protocols, and usage patterns—work in tandem with routers, which apply security rules and identify anomalous behavior based on published information about the devices.

Governments should drive a risk-based approach to trust and safety by considering all elements within the ecosystem, including software, firmware, and hardware deployed throughout IoT technologies, and avoiding device-centric policies that disrupt development and application of sophisticated network-based security measures.

IoT Security Policies Should Distinguish Between Consumer and Industrial IoT (IIoT)

Consumer IoT solutions—for example, wearables, smart home applications, and personal health monitoring devices—are generally targeted to individual users or families. They tend to be used in environments that are unmanaged or subjected to limited network administration, and that use minimal security services or none at all. These devices could last many years, but tend to be rapidly replaced with newer versions launched with the advent of new generations of technology.

Enterprise and industrial IoT technologies often function in highly managed environments using sophisticated network defenses.

The IIoT refers to the extension and use of the IoT in industrial sectors and applications. With a strong focus on M2M communication, big data, and machine learning, the IIoT targets existing automated industrial systems looking for dramatic improvements in productivity and efficiency, such as in large-scale factories or manufacturing plants. Other examples of IIoT technologies include connected HVAC systems, smart grid technologies, and interconnected medical devices in an operating room. Furthermore, commercial or enterprise technologies should generally be addressed by policies relating to industrial, rather than consumer, IoT. Enterprise IoT refers to applications in commercial office buildings, supermarkets, hotels, health care facilities, and retail stores, among others. Enterprise and industrial IoT technologies often function in highly managed environments using sophisticated network defenses. Additionally, policymakers may want to separately consider IIoT deployed in critical infrastructure sectors, due to the importance of these applications to national security, public health or safety, economic vitality, or any combination thereof.

Consumer IoT and IIoT solutions differ in their network environments, levels of risk, support life cycles, and complexity.

» **Network Environment.** Consumer IoT is used by the general public in their homes or offices. These users usually do not receive any cybersecurity training before the technology is deployed. Additionally, the equipment, such as home routers, and networks that consumer IoT connects to are rarely professionally managed. In contrast, IIoT solutions are usually deployed and maintained by in-house cyber professionals. The networks IIoT connects to are also in most cases managed by security experts deploying complex network defenses, since IIoT often supports critical industry functions.

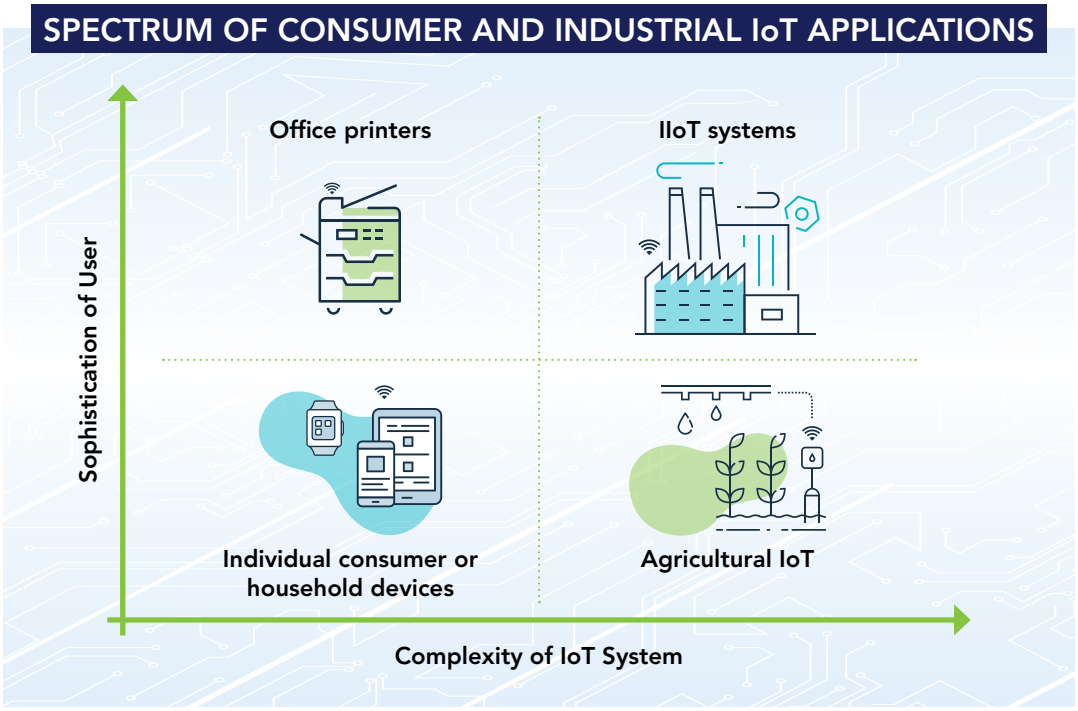
» **Risk.** Consumer IoT and IIoT present different security risks because these technologies are applied in drastically different environments. Common risks posed by consumer IoT include botnets, ransomware, and identity theft, since these solutions are often used by the average person on their home equipment and network. Because IIoT is often deployed in critical infrastructure environments, such as at manufacturing plants and power stations, IIoT security incidents risk equipment failure, loss of critical data, business and societal disruptions, or even injury and loss of life. The complexity of IIoT systems also provides a larger attack surface for malicious actors.

» **Support Life Cycle.** Technical security support for consumer IoT is relatively limited compared to IIoT. Consumer IoT solutions often implement security measures that are utility-centric, prioritizing the user experience and ease with which a consumer may use the product. Conversely, IIoT solutions often use advanced and robust security measures and protocols. Consumer IoT vendors may service their IoT devices, but consumers often do not have access to enterprise management tools and may replace devices every few years. Devices in the IIoT often require long-term investments in security, which include maintenance from in-house and field service technicians to sustain the levels of performance required by industrial systems. Additionally, IIoT sensors are often installed to measure parameters at remote infrastructure that is difficult to physically access, such as at oil and gas facilities located under the surface or offshore. Internal management capabilities can include sensor replacement, firmware upgrades, and management of gateways and server configurations, to name a few examples.

» **Complexity.** Consumer IoT products require less integration compared to IIoT solutions. IIoT systems are applied in complex environments with extensive legacy operations technology (OT). OT refers to the networking of operational processes and industrial control systems (ICSs), including human machine interfaces (HMIs), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and programmable logic controllers (PLCs). IIoT solutions must reliably integrate with these existing manufacturing systems, meaning patch management and other key security measures are much more complicated in these environments.

Consumer IoT and IIoT present different security risks because these technologies are applied in drastically different environments.

SPECTRUM OF CONSUMER AND INDUSTRIAL IoT APPLICATIONS



Policymakers should consider these important differences in consumer IoT and IIoT, and prioritize IoT security guidance and initiatives based on risk.

Governments should address the different risks posed by consumer IoT and IIoT technologies, rather than pursuing one-size-fits-all approaches. Policies for consumer devices may need to prioritize building security into devices, since consumers may not have the resources to create secure, managed environments; on the other hand, industrial users may need more flexibility to tailor security measures to their unique, complex operating environments.

IoT Security Policies Should Build on Industry Best Practices

Many technology companies are at the forefront of security innovation and with decades of experience developed best practices for IoT security. Many BSA members compete on security. However, not every business has the knowledge and expertise to make informed decisions about security when developing and deploying IoT technologies. Governments can enable better security outcomes by promoting best practices that range from security-by-design principles to sector-specific product development and risk assessment guides.

In particular, many best practices incorporate risk-based approaches to addressing security. Risk-based frameworks help policymakers, device manufacturers, and users understand and address the risks most likely to impact specific devices in the specific contexts in which they are used. Risk-based frameworks should incorporate analysis of risks to users (such as identity theft and reputational damage), to impacted systems or assets, including cybersecurity risks (such as disruption of key functions) and physical risks (damage to or destruction of physical systems), and to the broader ecosystem (such as cooption by a botnet or economic disruption). Risk-based frameworks should be the centerpiece of policy approaches to IoT security.

Industry consensus-building efforts have made significant progress in developing widely accepted IoT security guidance. For example, the BSA Framework for Secure Software[3] draws on best practices from leading enterprise software companies to provide software development organizations, their customers, and policymakers with guidance for assessing and encouraging security across the software life cycle, including the software that powers IoT solutions. Furthermore, the C2 Consensus on IoT Security Capabilities[4] brings together a group of 20 major cybersecurity and technology organizations to provide guidance to IoT device manufacturers on important security capabilities that IoT devices need to meet the market's expectations for security and harmonize policies around the world. Policymakers should look to these industry-developed guides to inform more effective IoT security policies that reduce fragmentation and promote good cyber hygiene among various industry sectors and parts of the IoT ecosystem.

Government IoT security policies should be informed by the expertise of industry leaders and incorporate widely accepted, industry-developed, risk-based IoT security best practices to elevate the security of the entire IoT market.

[3] BSA Framework for Secure Software, https://www.bsa.org/reports/bsa-framework-for-secure-software.

[4] The C2 Consensus on IoT Security Baseline Capabilities, https://securingdigitaleconomy.org/projects/c2-consensus/.

IoT Security Policies Should Incentivize Security Throughout the IoT Life Cycle

Security should be built into every stage of an IoT solution's life cycle, from development to decommissioning. In addition to secure development and security-by-design approaches, long-term security requires a life cycle management approach for maintaining software, hardware, and firmware components and addressing vulnerabilities post-deployment. Vulnerabilities are often identified by independent security experts and others in research communities, and reported to vendors. As part of a holistic approach to product maintenance and vulnerability management, vendors should establish clear procedures for receiving and addressing such third-party reports. Security professionals have developed guidance and standards on coordinated vulnerability disclosure (CVD) programs[5] to address this critical need; all such programs should be aligned with the internationally recognized ISO/IEC 29147 and 30111 standards.

To improve security outcomes throughout the IoT life cycle, policymakers should incentivize businesses to voluntary establish CVD processes that (1) align with internationally recognized standards, particularly ISO/IEC 29147 and 30111; (2) avoid counterproductive requirements, such as artificial mitigation timelines; and (3) reflect a holistic approach to vulnerability management throughout the life cycle of the IoT solution.

End-of-life policies are also an essential part of a holistic approach to product maintenance and vulnerability management. End-of-life refers to the date a product supplied to end users is determined to be at the end of its useful life (from the vendor's point of view) and the vendor stops marketing, selling, or sustaining the product. The continued use of unsupported IoT products and services or the abrupt termination of support can have serious consequences, particularly because out-of-date IoT products are more likely to be vulnerable to hackers and bugs, which could create vulnerabilities for other systems connected to these IoT technologies.

To comprehensively address security throughout the IoT life cycle, policymakers should also incentivize businesses to voluntarily establish end-of-life policies that (1) are updated based on the latest projections regarding end-of-life and end-of-life dates for the IoT product or service; and (2) are flexible enough to allow for changing circumstances.

Governments should incentivize businesses to voluntarily establish CVD processes and end-of-life policies to promote security throughout the IoT life cycle.

In addition to secure development and security-by-design approaches, long-term security requires a life cycle management approach for maintaining software, hardware, and firmware components and addressing vulnerabilities post-deployment.

IoT Security Policies Should Embrace Multistakeholder Processes

IoT is a challenging policy area, as it is a quickly developing environment and its technology spans many industries and uses. As the IoT market rapidly evolves, many in industry, including BSA members, have been at the forefront of developing innovative and responsible security methods and practices in the IoT space. Governments can learn from and incorporate the expertise industry has developed by formulating IoT security policies through a multistakeholder process that is open, transparent, and consensus-

[5] For more on software vulnerability disclosure, see BSA Guiding Principles for Coordinated Vulnerability Disclosure, https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdf. On hardware vulnerability disclosure, see Center for Cybersecurity Policy and Law, "Improving Hardware Component Vulnerability Disclosure," https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure.

based. Additionally, a multistakeholder process allows policymakers to learn from and incorporate the perspectives of others focused on IoT, including consumer groups and academics.

A multistakeholder process can also bring together the various manufacturers, vendors, and consumers that develop, sell, and use IoT products. Even though IoT technology spans many industry sectors, all who develop and use IoT solutions should prioritize security to protect an entire IoT system against cyber threats. Participants in a collaborative approach to IoT security will have the opportunity to share best practices and lessons learned, encourage security dialog, and develop flexible, shared security solutions that can adapt and evolve as threats change over time. A collaborative approach, one that draws on the expertise and engagement of a wide range of stakeholders, is needed to develop effective and appropriate IoT security policies.

Governments should initiate, lead, and support multistakeholder activities and working groups, collaborate with industry and others to understand evolving threats, and develop best practices for IoT security based on existing, consensus-based guidelines.

IoT Security Policies Should Seek National and International Policy Harmonization

Numerous governments, including at the national level (Australia,[6] the European Union,[7] Japan,[8] Singapore,[9] and the United Kingdom[10]) and the state or provincial level (California[11] and Oregon[12] in the United States) have developed initiatives to address IoT security. As more governments rightly focus on this pressing issue, the risk of fragmentation among policies increases. National and international fragmentation in governments' IoT security policies is problematic because IoT solutions are inherently interconnected and interdependent, and because fragmented policies can cause difficulties for manufacturers selling similar products in different markets that may have divergent or contradictory requirements. Such outcomes can reduce competitiveness and stifle innovation, thus undermining the ability of users to access the most secure technologies.

As government approaches to IoT security take shape, multinational technology companies developing IoT devices and their components will face an increasingly complex landscape of policy guidance, regulatory requirements, and standards. Manufacturers of IoT solutions want to market their devices worldwide, no matter where the underlying code was developed or the devices were manufactured. Such

6 *See* Department of Home Affairs, *Draft Code of Practice: Securing the Internet of Things for Consumers*, https://www.homeaffairs.gov.au/reports-andpubs/files/code-of-practice.pdf.

7 *See* ENISA, *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot; *see also* ENISA, *IoT Security Standards Gap Analysis*, https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis.

8 *See* Ministry of Economy, Trade and Industry, *IoT Security Guidelines ver. 1.0 Formulated*, https://www.meti.go.jp/english/press/2016/0705_01.html.

9 *See* Infocomm Media Development Authority, *Guidelines: Internet of Things (IoT) Cyber Security Guide*, https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/consultations/open-for-public-comments/consultation-for-iot-cyber-security-guide/imda-iot-cyber-security-guide.pdf.

10 *See* Department for Digital, Culture, Media & Sport, *Code of Practice for Consumer IoT Security,* https://www.gov.uk/government/publications/code-of-practice-forconsumer-iot-security.

11 *See* SB-327 Information Privacy: Connected Devices (California Legislative Assembly, 2017–2018), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327.

12 *See* Enrolled House Bill 2395 (80th Oregon Legislative Assembly, 2019), https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled.

businesses will be harmed by national and international policy landscapes that are disjointed, incoherent, and conflicting; such an outcome will suppress innovation and competitiveness. Harmonizing approaches to IoT security is a critical goal for the global economy.

Government IoT security policies should be informed by, and to the extent possible, aligned with other similar efforts underway around the world.

IoT Security Policies Should Support the Development and Use of Internationally Recognized IoT Standards

Several internationally recognized technical security standards are applicable to IoT technologies. These security standards provide widely vetted, consensus-based information and guidance for defining and implementing effective security methodologies, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability. IoT standards promote interoperability across various use case deployments, vendors, sectors, and geographies, and will maintain the long-term viability of the IoT and encourage the equitable distribution of the benefits and security of IoT solutions. Employing greater interoperability and the use of open, voluntary, and widely available standards as technical building blocks for IoT devices will support greater user benefits, innovation, and economic opportunity.[13] Regulations, certifications, and other government policies on IoT should be grounded in consensus-based, internationally recognized security standards wherever they exist. Where IoT standards do not yet exist, policymakers should refrain from mandating technical approaches to IoT, and, instead, encourage industry, researchers, and other stakeholders to work together on the development of open, consensus-based standards that support interoperability. This can be done by supporting existing standards development committees and by funding academic research into areas where evolving standards will be required, such as M2M interoperability.

Government IoT security policies should be tied to global, voluntary, and consensus-based standards wherever they exist, support the development of new internationally recognized IoT security standards, and refrain from localized standards or certifications that diverge from international best practices.

IoT Security Policies Should Establish Baseline Security Requirements as Necessary and Appropriate

As governments develop IoT security policies, considering the complexities of the IoT ecosystem and the differences between consumer IoT and IIoT, policymakers may determine IoT security regulations are required in some areas—in these specific contexts, policymakers may wish to identify core security capabilities in security guidance. Core IoT security capabilities consist of activities related to cybersecurity that are recommended for manufacturers to address in all applicable IoT products. These activities can help

[13] Alignment with international standards can encourage broad adoption of a government's security initiative or policy. For example, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity is aligned with internationally recognized standards and used worldwide, as demonstrated by the Framework's four translations and five adaptations by international governments. For more information, see NIST, International Perspectives, https://www.nist.gov/cyberframework/international-perspectives; see also NIST, International Resources, https://www.nist.gov/cyberframework/international-resources.

manufacturers lessen the cybersecurity burden on IoT device customers, which in turn can reduce the prevalence and severity of IoT device compromises and attacks performed using compromised IoT devices.

Security capabilities must address the entire usable life cycle of the IoT device, including the manufacturing, deployment, usage, transfer of ownership, decommissioning, and eventual destruction of the IoT device. Therefore, necessarily different stakeholders and responsible parties exist across the entire usable life cycle.

Depending on the context, core IoT security capabilities policymakers may consider include encryption, patchability, identity management, root of trust, and a secure development life cycle (SDLC). Such baseline requirements should always be aligned with internationally recognized standards and remain sufficiently flexible to account for technological developments.

- **Encryption.** IoT technologies should be developed in accordance with an encryption strategy that defines what data should be encrypted and which encryption mechanisms should be used, depending on how the device is deployed and the inherent privacy and security risks with its use.
- **Patchability.** Particularly for consumer IoT products that are not expected to be used within a managed security environment, IoT technologies should be capable of receiving—either remotely or in-person—secure updates and security patches.
- **Identity Management.** IoT technologies that handle sensitive information or otherwise control access should support strong identity management and authentication, including by applying current industry best practices on passwords and other user credentials.
- **Root of Trust.** IoT technologies should as appropriate ground security mechanisms in roots of trust to achieve stronger security assurances. Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.
- **Secure Development Life Cycle.** BSA members have been industry leaders in developing the concept of the SDLC, which includes robust attention to security considerations during a product's development, management of security issues throughout the product's life cycle, and iterative learning to improve development processes based on analysis of vulnerabilities or flaws as they are discovered. An SDLC—including vendor commitments to embrace secure development best practices, manage supply chain risk, mitigate identified vulnerabilities, and address end-of-life considerations—is critical for hardware, firmware, and software elements of IoT devices. The BSA Framework for Secure Software provides guidance on SDLC elements for software.

To the extent policymakers determine risks necessitate IoT security policies include specific security requirements, core security capabilities, including encryption, patchability, identity management, root of trust, and secure development life cycle, should align with widely accepted international standards, which are regularly updated to keep pace with the latest technology and security practices.

Security capabilities must address the entire usable life cycle of the IoT device, including the manufacturing, deployment, usage, transfer of ownership, decommissioning, and eventual destruction of the IoT device.

PRIVACY AND IoT

Securing IoT data is critical for mitigating both security and privacy risks. As IoT devices proliferate markets worldwide, consumers' ability to meaningfully control their data becomes increasingly important. Data privacy best practices can reinforce security procedures and should be adapted to IoT environments, reflecting both the sensitivity of the collected data and the purpose for which it is used. While these principles focus on IoT security, policymakers should consider complementary approaches to protect consumers' privacy when using IoT technologies. Comprehensive approaches to data privacy, which encompass data collected by IoT applications, can help ensure technologies safeguard consumers' privacy.

IoT Security Policies Should Integrate Security Into IoT Acquisition

As consumer and industry IoT technologies become more pervasive in the coming years, government use of IoT solutions is also expected to increase. In developing procurement guidelines and setting policies for measuring supply chain risks that are informed by information-driven, risk-based analysis, agencies can positively affect the cybersecurity of civilian government. Equally critical, prioritizing security in IoT procurement can benefit consumers by incentivizing the broader IoT market to produce more secure products.

Policymakers considering stronger procurement practices for IoT devices, platforms, and services should ensure that policies are aligned with available internationally recognized standards and emphasize adherence to best practices in security. Secure solutions, with multi-layered hardware- and software-level capabilities, should therefore be a procurement priority for government IoT.

Governments should incentivize departments and agencies in the procurement process to prioritize secure, interoperable, and scalable IoT solutions for assets based on voluntary, industry-led, consensus-based, global guidelines.

IoT Security Policies Should Factor IoT Into Incident Response

As IoT applications proliferate and deliver benefits to consumers and industrial users, governments should factor IoT into incident and emergency responses. Responding to and resolving large-scale IoT incidents can be especially challenging, given that IoT attacks can be complex and dynamic, and may involve cyber and physical threats. Policymakers must incorporate IoT considerations into the development of incident response plans and policies, which should address the potential speed and scale of IoT attacks. Additionally, policymakers should consider how IoT technologies can improve emergency planning and responses, including through mission-critical logistics support and communications, emergency calling, and public warning systems.

Governments should integrate IoT into incident response planning, including policies and programs for IoT incidents and emergency responses.

IoT technologies are rapidly transforming daily lives and business processes. As IoT solutions become more ubiquitous, policymakers will need to act swiftly to promote security throughout the IoT ecosystem. Representing leaders in cybersecurity and IoT innovation, BSA strongly supports responsible, risk-based approaches to IoT security. The principles outlined above will guide governments in tackling this complex policy issue, and BSA would welcome opportunities to collaborate with policymakers in driving security throughout the IoT marketplace.

Key Resources

BSA | The Software Alliance, *The BSA Framework for Secure Software*, April 29, 2019. https://www.bsa.org/reports/bsa-framework-for-secure-software.

Charter of Trust, *Charter of Trust Principles*. https://www.charteroftrust.com/wp-content/uploads/2020/02/200212_Dok-Narrative_A4_EN_200212.pdf.

Cisco, *Cisco Annual Internet Report (2018–2023)*, March 2020. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

Council to Secure the Digital Economy, *The C2 Consensus on IoT Security Baseline Capabilities,* September 17, 2019. https://securingdigitaleconomy.org/projects/c2-consensus/.

Department of Defense, *DoD Policy Recommendations for The Internet of Things (IoT)*, December 2016. https://www.hsdl.org/?view&did=799676.

European Telecommunications Standards Institute, *EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations*, July 2019. https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf.

European Union Agency for Cybersecurity, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, November 29, 2018. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

Intel, Internet of Things Policy Framework. https://www.intel.com/content/www/us/en/policy/policy-iot-framework.html.

International Organization of Standardization, *Information Technology – Cloud computing – Overview and vocabulary*, ISO/IEC 17788 (2014).

International Organization of Standardization, *Information Technology – Cloud computing – Edge computing landscape*, ISO/IEC 23188 (2020).

International Organization of Standardization, *Information Technology – Internet of Things (IoT) – Vocabulary*, ISO/IEC 20924 (2019).

International Organization of Standardization, *Information technology – Security techniques – Application security; Parts 1–7*, ISO/IEC 27034 (1:2011-7:2018).

International Organization of Standardization, *Information technology – Security techniques – Vulnerability disclosure*, ISO/IEC 29147 (2019).

International Organization of Standardization, *Information technology – Security techniques – Vulnerability handling processes*, ISO/IEC 30111 (2019).

International Organization of Standardization, *Internet of things (IoT) – Interoperability for internet of things systems – Part 1: Framework*, ISO/IEC 21823-1 (2019).

International Organization of Standardization, *Internet of Things (IoT) – Reference Architecture*, ISO/IEC 30141 (2018).

Microsoft, *Cybersecurity policy for the Internet of Things*. https://www.microsoft.com/en-us/cybersecurity/content-hub/iot-cybersecurity-policy.

Microsoft Research NExT Operating Systems Technologies Group, *The Seven Properties of Highly Secure Devices*, March 2017. https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf.

National Institute of Standards and Technology, NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*, May 29, 2020. https://www.nist.gov/publications/foundational-cybersecurity-activities-iot-device-manufacturers.

National Institute of Standards and Technology, NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline*, May 29, 2020. https://www.nist.gov/publications/iot-device-cybersecurity-capability-core-baseline.

PTC, *The State of Industrial Internet of Things 2019: Spotlight on Operational Effectiveness*, 2019. https://www.ptc.com/-/media/Files/PDFs/IoT/State-of-IIoT-Report-2019.pdf.